

A Technology Comparison

AV, IDS/IPS and Damballa's Response to Targeted Attacks

Introduction

It is a very reasonable question:

If all of the network security defenses, policies and procedures that we can reasonably be expected to deploy are in place and working, *how are targeted attacks still getting through?*

After all, antivirus (AV) and intrusion detection/intrusion prevention systems (IDS/IPS) are mature, stable technologies that are very effective at stopping the threats they were designed to address. They stop viruses and worms. They recognize the inappropriate activity associated with those attacks. They recognize and stop overt, aggressive brute force attacks that attempt to force their way in through the network perimeter. These security tools, in short, are an essential, proven investment, and ones certainly worth maintaining. They may not stop targeted attacks, but they still reduce the overall number of threats facing a typical enterprise network by 90% or more.

The irony is that the very success of AV and IDS/IPS is one of the key reasons targeted attacks can so easily evade them. Consider BotArmies, one of the most rapidly growing delivery mechanisms for targeted attacks. BotArmies, also called botnets or zombie networks, require three components to operate:

Malware – Malicious software code that either executes like a program or alters the configuration of its host, so that the machine is under the remote control of an unauthorized third-party.

Controller – An individual or an organization that creates and controls networks of compromised computers across corporate and national boundaries, and then uses these systems for illegal activities.

Command-and-Control (CnC) – a system spanning the Internet used to send instructions to compromised computers and to retrieve stolen data, as well as hide the controller's identity and location.

The malware component is the part of a targeted attack that a reasonable person would expect AV to stop, either before a system can be co-opted or before malicious activity can affect the enterprise. However, Damballa's own experience shows that 3%-5% of enterprise systems are already compromised, even when AV and IDS/IPS are fully deployed and working as expected.

Targeted attack malware is different from viruses, worms and Trojan horses. It is created by professional criminal organizations for the express purpose of generating money. Stealth and stability, therefore, are prime motivations behind the creation and distribution of the malware. Compromised systems can be given new instructions or

even completely new application code as often as every 30 minutes. And yet, the best AV vendors require anywhere from half a day to a month or more to identify a new threat and update their products accordingly. It takes even longer to distribute those updates across the enterprise. AV simply can't keep up.

AV focuses primarily on the file system of the host. Malware authors take advantage of this fact by constantly changing how the malware is represented within the file system. As a result, targeted attack malware can hide itself quite successfully. For example, AV cannot detect attacks that:

- Are intermittent rather than constant, which hides the overall level of activity
- Mimic legitimate applications and allow normal use of the compromised system
- Use communications ports that must be left open to allow Web and email traffic
- Attach themselves to user-level applications but maintain normal capabilities
- Disable AV so that it appears effective, even though it is not doing anything
- Install *under* the operating system (rootkits), so that no software application can identify their presence or activity¹

Targeted attacks, therefore, are a fundamentally different type of security challenge, one that signature-based defenses such as AV and IDS/IPS are not designed to address. That is why these attacks represent the worst of the worst – the threats that slip through, no matter how up-to-date the security technology might be. These BotArmies may only represent 10% percent of the overall online threats facing an enterprise, but they are the security exposures most likely to deliver expensive, embarrassing and ongoing damage.

Numerical Proof

Consider an enterprise network with 25,000 systems. 90% of these computers are likely to run some variety of Microsoft Windows, and 80% of these Windows systems typically grant full administrator rights to at least one user, which means that this user has unlimited access to all aspects of the operating system.

At the network level, firewalls block all traffic except HTTP (Web) and HTTPS (encrypted Web). Proxy servers aggregate, monitor and cache network traffic to better manage traffic flow and monitor proper usage of network resources. Corporate AV and IDS/IPS solutions are deployed and kept completely up-to-date.

This network is almost certainly compromised by BotArmy-driven targeted attacks. In fact, Damballa's technology can be expected to find that ***between 17 and 87 of this enterprise's systems either carry targeted attack malware or are communicating with confirmed malicious controllers across the Internet*** during a standard 30-day

¹ According to Damballa's research, only about 35% of current malware contains rootkit capabilities. However, rootkits are very difficult to identify or remediate, and usually require that the compromised hard drive be destroyed

evaluation. Every one of these systems is operating outside of IT's control, and the non-Damballa parts of the security solution cannot detect the security breach.

These numbers are very conservative. They assume that:

- 35% of targeted attack malware requires administrator access to function
- 78% of targeted attack malware uses HTTP ports for communications with other elements of the BotArmy
- 60% (or more) of targeted attack malware will never be caught by any signature-based AV or IDS/IPS solution²

For many organizations with less stringent security practices, the actual level of targeted attack penetration is probably much worse.

Why Damballa Finds What Others Miss

Damballa's security solutions take a completely different approach to identifying targeted attacks and isolating compromised systems within the enterprise. All targeted attacks need one constant in order to turn individual compromises into a coordinated attack army – Command-and-Control (CnC). Everything else – the malware, the target, the location of the compromised host – can (and does) change. But something has to remain constant so that instructions can be sent and stolen information returned.

Damballa isolates targeted attack CnC from legitimate Internet traffic, and then uses this insight to identify malicious and suspicious communications between internal enterprise systems and the external controllers operating a targeted attack's BotArmy. This information makes it possible to identify a compromised system with very high confidence and very few false positives, even in the absence of actual malware identification or known malware behavior.

In short, Damballa separates the malicious signal from the background noise of the Internet whenever a compromised system attempts to "phone home" across the Internet. Damballa also distinguishes between basic CnC traffic and active attacks, which helps security administrators and IT staff calibrate their response to the information that Damballa discovers. This technology is fundamentally different from the model used by AV and IDS/IPS, and is why Damballa is so accurate at finding compromised hosts in real-time.

The practical result is that Damballa can see targeted attacks that AV, IDS/IPS or anything else cannot. The following table summarizes the key differences between Damballa and signature-based defenses, such as AV and IDS/IPS:

² These figures are based on Damballa's actual experience inside enterprise networks operating in normal production environments, plus active ongoing evaluations of corporate AV products and their ability to identify newly discovered targeted attack malware

	Damballa	AV	IDS/IPS
Protects against Zero-Day threats	YES	No	No
Protects without signatures	YES	No	No
Few, if any, false positives	YES	Yes	No
Multiple types of analysis	Dozens	Generally only 1 in terms of actual use	Generally only 1 in terms of actual use
Provides protection without end-point agents	YES	No	Yes
Doesn't slow network or individual systems	YES	No	Yes
Protects immediately against any new versions of malware code	YES	Delay of days to months	Delay of days to months
Identifies malicious activity, even in the absence of malware (Zero-Day attacks)	YES	No	No
Protects against low volume/intermittently active attacks	YES	No	No
Protects against compromises that originate from mobile or remote systems	YES	Only if all systems fully patched and security agents updated	Yes
Protects itself from malware attacks	YES	No	Yes
Identifies targeted attack activity masquerading as legitimate applications	YES	No	No – seeks broad-based attacks, not targeted attacks
Identifies targeted attack activity using common, always-open ports (HTTP, HTTPS, FTP, etc.)	YES	No	Yes for broad-based attacks, but will not stop a targeted attack
Identifies encrypted targeted attack activity	YES	N/A	No

Conclusion

As long as the Internet is a conduit for business, attackers will attempt to leverage it for illegal and highly profitable activities. Enterprise organizations have responded to these threats, and attackers have learned how to evolve viruses, worms and Trojan horses into much more sophisticated forms of targeted attack. As a result, traditional network security infrastructure needs to be supplemented with new solutions such as Damballa, which deliver protection against attacks that other solutions cannot see and cannot stop. This enhanced level of protection closes the gap between when signature-based solutions end and where true enterprise protection needs to be.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation of malicious activity. Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa is privately held and headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo and Harvester. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.